September 2024
12. Jahrg.
Seite 89 – 180

RAW

2

Recht ■ Automobil ■ Wirtschaft
Unternehmen | Technologie | Beratung

dfv Mediengruppe · Frankfurt am Main

3. Sanktionen für Unternehmen und Direkthaftung von Leitungspersonen

Zur Durchsetzung der Vorgaben sehen die Artt. 32 ff. neben Aufsichts- insbesondere Sanktionsmaßnahmen vor, die wirksam, verhältnismäßig und abschreckend ausgestaltet sein sollen. Gegenüber wesentlichen Einrichtungen soll bei Nichtbefolgen behördlicher Anweisungen gem. Art. 32 Abs. 5 UAbs. 1 S. 2 lit. a) als ultima ratio vorübergehend die Betriebsgenehmigung und Zertifizierung ausgesetzt oder gem. Art. 32 Abs. 5 UAbs. 1 S. 2 lit. b) die Tätigkeit von Personen auf der Geschäftsführungs- oder Vorstandsebene untersagt werden können.[81]

Als zusätzliches Sanktionsmittel sieht die NIS2-Richtlinie Bußgelder vor, die an das Konzept in der DSGVO erinnern.[82] Bei Verstößen gegen die Risikomanagementmaßnahmen und Berichtspflichten soll das mögliche Bußgeld gem. Art. 34 Abs. 5 für wichtige Einrichtungen bis zu 7 000 000 Euro oder 1,4 % des Jahresumsatzes und für wesentliche Einrichtungen gem. Art. 34 Abs. 4 sogar bis zu 10 000 000 Euro oder 2 % des Jahresumsatzes erreichen können.[83]

Neben den behördlichen Sanktionsmitteln sieht die NIS2-Richtlinie zudem eine zivilrechtliche persönliche Einstandspflicht der Leitungspersonen vor. Art. 32 Abs. 6 verlangt die Kodifizierung einer Haftungsgrundlage, nach der die verantwortlichen Personen oder Vertreter des Unternehmens für Verstöße gegen ihre Pflichten haftbar gemacht werden können. Die Mitgliedstaaten müssen folglich eine persönliche Schadensersatzhaftung der Unternehmensverantwortlichen für die Missachtung der Cybersicherheitspflichten sicherstellen.[84]

IV. Fazit

Vor dem Hintergrund der stetigen Weiterentwicklung der Technologien in der Automobilindustrie stellt die NIS2-Richtlinie auch eine regulatorische Antwort auf die zunehmenden Cyberrisiken in diesem Bereich dar. In der Branche werden sowohl Hersteller als auch Zulieferer prüfen müssen, ob sie in den Anwendungsbereich der Richtlinie fallen, was sich mitunter als Herausforderung erweisen kann. Betroffene Unternehmen werden gewährleisten müssen, dass sie ein effektives CSMS einrichten und den Meldepflichten bei erheblichen Sicherheitsvorfällen nachkommen. Dabei haben sie sicherzustellen, dass Mitarbeiter und Leitungspersonen über ausreichende Kenntnisse im Bereich der Cybersicherheit verfügen, um die Anforderungen effektiv zu erfüllen und dabei empfindliche Sanktionen zu vermeiden. Auch wenn nicht alle Mitgliedstaaten bis zum Ende der Umsetzungsfrist NIS2-Umsetzungsgesetze verabschiedet haben werden, sollten Unternehmen der Automobilindustrie bereits jetzt die notwendigen Maßnahmen ergreifen, um Cybersicherheitsrisiken für ihre geschäftskritischen Systeme zu minimieren, Datenintegrität und Produktsicherheit zu gewährleisten und sich so für die Cyberherausforderungen der Zukunft zu rüsten.

V. Summary

Against the backdrop of the continual advancement of technologies in the automotive industry, the NIS2 Directive is also a regulatory response to the increasing cyber threats in this sector. Both manufacturers and suppliers in the industry will need to assess whether they fall within the scope of the Directive, which can sometimes prove challenging. Affected companies will need to ensure that they establish an effective CSMS and comply with the reporting obligations for significant security incidents. In doing so, they must ensure that employees and management personnel possess sufficient knowledge in the field of cybersecurity to meet the requirements effectively and to avoid fines that can amount to millions. Even if not all member states will have enacted NIS2 implementation laws by the end of the transposition period, automotive industry companies should already be taking the necessary measures to mitigate cybersecurity risks to their business-critical systems, ensure data integrity and product safety, and prepare themselves for the cyber challenges of the future.

81 Dies soll nach § 63 Abs. 9 S. 3 NIS2UmSuCG-E nur zulässig sein, wenn und solange eine „besonders wichtige Einrichtung" den Anordnungen des BIS trotz Fristsetzung nicht nachkommt.

82 *Blum/Adelberg*, CB 2024, 145, 146; zum Verhältnis bei mitverwirklichten Datenschutzverstößen, s. *Ritter*, RDV 2023, 152, 158.

83 Gem. § 67 Abs. 5 S. 1 Nr. 3 NIS2UmSuCG-E soll das Bußgeld über den Verweis des § 61 Abs. 5 S. 2 NIS2UmSuCG-E auf § 30 Abs. 2 S. 3 OWiG bis zu 20 000 000 Euro betragen können, wenn das Unternehmen einer vollziehbaren Anordnung zuwiderhandelt.

84 Während der vormalige Entwurf – in überschießender Umsetzung – den Verzicht auf Ersatzansprüche gegenüber Leitungspersonen noch für unwirksam erklärte, sieht der derzeitige Entwurf die Anwendung des allgemeinen Gesellschaftsrechts vor, es sei denn es ist in den „für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten", § 38 Abs. 2 NIS2UmSuCG-E.

Dr. Cathrin Wentzel, LL.M. (University of Sussex) und Benedikt Lutz, LL.M.*

Zugangsanspruch zu Reparatur- und Wartungsinformationen nach der Typgenehmigungsverordnung und Data Act – eine Gegenüberstellung

I. Vorspann

Der Zugang zu Daten ist gerade im Automotive- und Mobilitätsbereich heiß umkämpft und entwickelt sich in rasanter Geschwindigkeit fort.

Ab dem 14.4.2025 müssen Betreiber und Eigentümer von öffentlich zugänglichen Ladepunkten und Zapfstellen für alternative Kraftstoffe gemäß Art. 20 ARFID[1] bestimmte

* Mehr über die Autoren erfahren Sie auf S. III und IV.

1 Verordnung 2023/1804.

Daten öffentlich und kostenfrei zur Verfügung stellen. Dazu gehören etwa die geografische Lage der Ladepunkte, die Komptabilität des Fahrzeugtyps und der aktuelle Preis.

Mit der am 18.10.2023 in Kraft getretenen RED III-Richtlinie[2] wurden Regelungen zur Bereitstellung von Informationen für Batteriehersteller erlassen. Gemäß Art. 20a Abs. 3 RED III-RL sollen Hersteller von Batterien kostenlos Echtzeitzugang zu Batteriemanagementsysteminformationen gewähren. Dazu gehören etwa Batteriekapazität, Alterungszustand und Leistungseinstellung. Aktuell ist die RED III-RL noch nicht in Deutschland umgesetzt.

Schließlich hat die Bundesregierung Ende Juli 2023 das Eckpunktepapier für ein neues Mobilitätsdatengesetz vorgelegt.[3] Das Gesetz soll bis Ende 2024 verabschiedet werden.[4] Ziel ist es, eine freie Zugänglichkeit von Mobilitätsdaten sicherzustellen.[5]

Im Automotivebereich gibt es allerdings bereits seit vielen Jahren Regelungen zum Zugang bzw. Regelungen zur technischen Ausgestaltung des Datenzugangs in Bezug auf bestimmte Daten und Informationen.[6]

Eine zentrale Rolle kommt dabei der Typgenehmigungsverordnung[7] zu (nachfolgend „VO 2018/858"), die unter anderem Regelungen zur Bereitstellung von OBD-Daten oder zum Zugang zu Reparatur- und Wartungsinformationen enthält.[8]

In Zukunft wird neben den sektorspezifischen Datenzugangsansprüchen auch der Data Act eine herausragende Rolle im vernetzten Fahrzeug spielen.[9] Der Data Act enthält neben konkreten Datenzugangsansprüchen in Bezug auf nutzergenerierte Daten auch allgemeine Vorgaben zur Ausgestaltung von Datenzugangsansprüchen (Art. 8 ff. DA) und zu Verträgen über die Nutzung und den Zugang von Daten (Art. 13 DA). Dieser Beitrag stellt die Regeln zum Zugang zu Wartungs- und Reparaturinformationen nach Art. 61 f. der VO 2018/858 (nachfolgend „RMI-Daten") gegenüber und bewertet die möglichen Auswirkungen des Data Act auf die Zugangsregeln nach der VO 2018/858.

II. Vergleich der Zugangsregelungen (Data Act/ Zugang zu RMI-Daten)

1. Normadressat und Anspruchsberechtigter?

a) Zugang zu RMI-Daten nach der VO 2018/858

Ziel der Art. 61 f. der VO 2018/858 ist es, den Wettbewerb auf den Aftersales-Märkten zu gewährleisten.[10]

Art. 61 Abs. 1 der VO 2018/858 nimmt dafür die Hersteller im Sinne des Art. 3 Nr. 40 der VO 2018/858 als Normadressaten in die Pflicht. Diese müssen sogenannten „*unabhängigen Wirtschaftsakteuren*" Zugang zu u. a. RMI gewähren. „*Unabhängige Wirtschaftsakteure*" sind in Art. 3 Nr. 45 der VO 2018/858 definiert. Der Begriff umfasst danach zum Beispiel freie Werkstätten, Händler und Hersteller von Werkstattausrüstung, Ersatzteilen oder Diagnosegeräten und auch sogenannte „*Herausgeber von technischen Informationen*".[11]

Solche Herausgeber sind etwa Unternehmen, die RMI mehrerer Hersteller zusammentragen und interessierten Reparaturbetrieben konsolidiert bereitstellen. Tatsächlich lag ein Augenmerk des europäischen Gesetzgebers gerade darauf, auch solche Wirtschaftsakteure zu berücksichtigen, die keine Reparaturbetriebe sind, um auch den Wettbewerb auf dem „Markt für Fahrzeugreparatur- und Fahrzeugwartungsinformationsdienste" zu fördern.[12]

Der Katalog der in Art. 3 Nr. 45 VO 2018/858 genannten unabhängigen Wirtschaftsakteure ist nicht abschließend. Erfasst sind ferner alle „*natürliche[n] oder juristische[n] Person[en], die kein Vertragshändler oder keine Vertragswerkstatt [sind] und direkt oder indirekt an der Wartung und Reparatur von Fahrzeugen beteiligt [sind]*". Autorisierte Vertragshändler und -werkstätten sind hingegen als Anspruchsberechtigte ausgeschlossen, jedenfalls soweit RMI-Daten im Zusammenhang mit Fahrzeugen des Herstellers betroffen sind, für den diese tätig sind. Hingegen kann ein autorisierter Betrieb für „Marke A" als unabhängiger Wirtschaftsakteur Zugang nach Art. 61 Abs. 1 der VO 2018/858 gegenüber dem Hersteller von „Marke B" verlangen.

b) Data Act

(1) Normadressat

Hinsichtlich der Zugangsansprüche nach dem Data Act ist zu differenzieren. So stellt der Access by Design Anspruch gemäß Art. 3 Abs. 1 DA im Grunde auf den Hersteller bzw. Entwickler des vernetzten Produktes sowie den Anbieter des verbundenen Dienstes ab. Der Hersteller des vernetzten Produktes muss bei der Entwicklung dafür Sorge tragen, dass dieses „*so konzipiert und hergestellt*" wird, dass „*die Produktdaten und verbundenen Dienstdaten […] direkt zugänglich sind*".[13] Das Gleiche gilt für verbundene Dienste.

Normadressaten des Zugangsanspruchs nach Art. 4 Abs. 1 DA und Art. 5 Abs. 1 DA ist der jeweilige Dateninhaber. Der Dateninhaber ist nach Art. 2 Nr. 13 DA diejenige Person, die nach dem Data Act, „*nach geltendem Unions-*

2 Richtlinie 2023/2413.
3 BMVD, BMDV startet Prozess für ein Mobilitätsdatengesetz, 28.10. 2022, BMDV – BMDV startet Prozess für ein Mobilitätsdatengesetz (bund.de) (Abruf: 15.7.2024).
4 BMVD, BMDV startet Prozess für ein Mobilitätsdatengesetz, 28.10. 2022, BMDV – BMDV startet Prozess für ein Mobilitätsdatengesetz (bund.de) (Abruf: 15.7.2024).
5 Eckpunkte Mobilitätsdatengesetz S. 1.
6 Siehe etwa Art. 4 VO 2022/545 in Bezug auf den Umgang mit bestimmten Daten und Informationen im Zusammenhang mit dem Ereignisdatenspeicher des Fahrzeugs; vgl. zudem etwa Art 61 ff. VO 2018/858 hinsichtlich des Zugangs zu insbesondere Reparatur- und Wartungsinformationen.
7 VO 2018/858 des Europäischen Parlaments und des Rates v. 30.5. 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbst-ständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen Nr. 715/2007 und Nr. 595/2009 und zur Aufhebung der RL 2007/46/EG.
8 Im nachfolgenden werden Reparatur- und Wartungsinformationen gem. Art. 61 Abs. 1 der VO 2018/858 „RMI" bzw. „RMI-Daten" genannt.
9 VO 2023/2854 des Europäischen Parlaments und des Rates v. 13.12. 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung). Im Folgenden „Data Act" oder „DA".
10 ErwG 50 und 52 der VO 2018/858.
11 Art. 3 Nr. 45 und ErwG 52 der VO 2018/858; EuGH Urt. v. 27.10.2022 – C-390/21, BeckRS 2022, 28847.
12 ErwG 52 der VO 2018/858; vgl. auch Art. 61 Abs. 2 der Typgenehmigungsverordnung.
13 Art. 3 Abs. 1 DA.

recht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen […]". Diese Definition wird oft als Zirkelschluss bezeichnet[14] und bringt in der Tat keinen großen Erkenntnisgewinn.[15] Allerdings liegt der Definition eine einfache Logik zugrunde: Nur wer tatsächlich Zugriff auf diese Daten hat, kann den Zugangsanspruch auch gewähren. Folglich ergibt sich aus der Gesamtschau der Regelungen, dass der Dateninhaber derjenige ist, der faktisch die Kontrolle über die relevanten Daten hat.[16]

Dementsprechend wird der Dateninhaber bei vernetzten Produkten, wie etwa Fahrzeugen, oftmals der Hersteller des vernetzten Produktes und bei verbundenen Diensten der Anbieter des verbundenen Dienstes sein.[17]

(2) Anspruchsberechtigter

Anspruchsberechtigte sind die Nutzer der vernetzten Produkte und der verbundenen Dienste. Wer Nutzer ist, ist in Art. 2 Nr. 12 DA legaldefiniert: „[E]*ine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt.*" In den Erwägungsgründen des Data Act wird dies wie folgt konkretisiert: „[D]*ie Eigentümer eines vernetzten Produkts oder – beispielsweise durch einen Miet- oder Leasingvertrag – Inhaber bestimmter befristeter Rechte auf Zugang zu Daten aus dem vernetzten Produkt oder auf deren Nutzung ist oder verbundene Dienste für das vernetzte Produkt in Anspruch nimmt.*"[18] Daher ist davon auszugehen, dass sowohl die Eigentümerstellung als auch die berechtigte Nutzung die Nutzereigenschaft begründen.[19] Ein unberechtigter Besitz führt dagegen nicht zu einer Nutzerstellung.[20]

Bei verbundenen Diensten wird der Nutzer in der Regel derjenige sein, mit dem der Dateninhaber einen Vertrag über die Nutzung des verbundenen Dienstes abschließt.

Bei vernetzten Produkten wird es bei dieser recht weiten Definition in vielen Fällen, gerade auch bei Fahrzeugen, oftmals mehrere Nutzer geben. So wird z. B. bei Leasingfahrzeugen sowohl der Leasinggeber als Eigentümer als auch der Leasingnehmer als schuldrechtlich Berechtigter Nutzer im Sinne des Data Act. Im Einzelfall kann ein einzelnes Produkt nach dieser Definition viele unterschiedliche Nutzer haben, etwa bei einem Car-Sharing Dienst.[21] Hier wäre sowohl der Car-Sharing Anbieter Nutzer als auch jeder, der den Car-Sharing Dienst aufgrund eines entsprechenden (Miet-)Vertrages nutzt – auch wenn die Nutzung ggf. nur wenige Minuten dauert.[22] Teileweise wird daher eine gewisse Erheblichkeitsschwelle der Nutzung gefordert.[23]

Dritte haben grundsätzlich keinen eigenständigen Anspruch auf einen Datenzugriff. Allerdings formuliert Art. 5 Abs. 1 DA die Möglichkeit, dass Nutzer die Weitergabe ihrer Daten an Dritte vom Dateninhaber verlangen können. Dritter kann grundsätzlich jeder sein, nicht aber Gatekeeper i. S. d. Art. 3 DMA.[24]

Dritte können daher insbesondere auch „unabhängige Wirtschaftsakteure" im Sinne von Art. 3 Nr. 45 der VO 2018/858, wie etwa Reparaturbetriebe oder Herausgeber von technischen Informationen sein.

2. Gegenstand des Zugangsanspruchs

a) Zugang zu RMI-Daten nach der VO 2018/858

Art. 61 der VO 2018/858 eröffnet u. a. Zugang zu „*Fahrzeugreparatur- und -wartungsinformationen*" der Hersteller.[25]

Der Begriff „*Fahrzeugreparatur- und -wartungsinformationen*" ist weit zu verstehen. Er umfasst nach Art. 3 Nr. 48 der VO 2018/858 insbesondere alle Informationen, betreffend die Reparatur, die Instandhaltung und Inspektion und die Diagnose eines Fahrzeugs, wie etwa Ersatzteilinformationen oder die Fahrzeugidentifikationsnummer (FIN),[26] wenn und soweit diese Informationen hierfür „*erforderlich*" *sind*.[27] Art. 61 Abs. 1 und 4 i. V. m. den Ziffern 2.5 und 6.1 des Anhang X der VO 2018/858 stellen hierbei eine Übersicht an verschiedenen Typen von RMI-Daten bereit.

In der VO 2018/858 findet sich keine Eingrenzung dahingehend, wie RMI-Daten entstehen. Der Gesetzgeber geht jedoch implizit davon aus, dass – jedenfalls im Ausgangspunkt – typischerweise nur der Hersteller des Fahrzeugs aufgrund des Entwicklungs- und Herstellungsprozesses über diese Daten verfügt.[28] Daher stützen sich die RMI-Datenzugangsregeln auf die Prämisse, dass der Hersteller die RMI-Daten auch an unabhängige Wirtschaftsakteure herausgeben muss, die er seinen autorisierten Betrieben bereitstellt und/oder selbst im Bereich Aftersales nutzt.[29] Verfügt der Hersteller außerdem auch über sogenannte Wartungsaufzeichnungen, hat er diese unabhängigen Werkstätten kostenlos bereitzustellen, Art. 61 Abs. 9 der VO 2018/858.

Dem Zugangsanspruch können auch solche Daten unterfallen, die bei der Nutzung des Fahrzeugs generiert werden, z. B. bestimmte Sensordaten. Hinsichtlich der OBD-Daten ist dies ausdrücklich in Art. 61 Abs. 1 der VO 2018/858 geregelt. Jedoch ist auch denkbar, dass andere fahrzeuggenerierte Daten der weiten Definition der RMI-Daten unterfallen und damit Gegenstand der Zugangsregeln werden. Dies dürfte auch der Auffassung der Kommission entsprechen. Diese führt in den ergänzenden Kfz-Leitlinien[30] aus, dass sie fahrzeuggenerierte Daten als

14 *Bomhard/Merkle*, RDi 2022, 168, 169; *Kaesling* GRUR 2024, 821, 827; *Wunner* ZUM 2024, 424, 430.
15 *Heinzke/Herbers/Kraus*, BB 2024, 649, 649.
16 *Heinzke/Herbers/Kraus*, BB 2024, 649, 649.
17 Ebenso *Ziegler/Nagl*, ZfDR 2023, 57, 67.
18 ErwG 18 S. 1, 5; ErwG 21 S. 1.
19 *Kaesling*, GRUR 2024, 821, 822.
20 *Specht-Riemnschneider* MMR 2022, 809, 813 f.
21 *Etzkorn*, RDi 2024, 116, 117; ErwG 1.
22 Ähnlich auch *Schild*, in: BeckOK Datenschutzrecht, Data Act, 1.5. 2024, Art. 2 DA, Rn. 76.
23 *Antoine*, CR 2024, 2, 4.
24 *Hennemann/Steinrötter*, NJW 2024, 1, 4.
25 Neben dem Zugang zu RMI-Daten müssen Hersteller den unabhängigen Wirtschaftsakteuren auch z. B. On-Board-Diagnosedaten (OBD-Daten), Diagnose- und andere Geräte und Instrumente (inkl. Referenzinformationen und Software) bereitstellen.
26 EuGH, Urt. v. 9.11.2023 – C-319/22, GRUR-RS 2023, 30962 (Rn. 62) – Scania.
27 Vgl. zur Frage der Erforderlichkeit Hübener/Lutz ZWeR 2024, 130.
28 Vgl. ErwG 52 VO 2018/858.
29 Art. 3 Nr. 48 VO 2018/858.
30 Ergänzende Leitlinien für vertikale Beschränkungen in Vereinbarungen über den Verkauf und die Instandsetzung von Kraftfahrzeugen und den Vertrieb von Kraftfahrzeugersatzteilen (2010/C 138/05), geändert durch Anpassungen vom 17.4.2023 (2023/C 133 I/01).

„technische Informationen“[31] im Sinne der VO 461/2010 und der Kfz-Leitlinien betrachtet, wenn diese für die Instandsetzung und Wartung von Fahrzeugen „*von wesentlicher Bedeutung*“ seien.[32, 33]

b) Data Act

Kapitel II des Data Acts über die „*Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen*“ gilt für alle Daten in Rohform und vorverarbeitete Daten, die aus der Nutzung eines vernetzten Produkts oder eines damit verbundenen Dienstes generiert werden. Dies gilt sowohl für personenbezogene als auch für nicht-personenbezogene Daten, einschließlich relevanter Metadaten.[34]

Zwar spricht die Definition von „Produktdaten“ in Art. 2 Nr. 15 DA von Daten, die „*bei der Nutzung eines vernetzten Produktes*“ generiert werden. Darauf soll es aber nach Erwägungsgrund 15 gerade nicht ankommen. Dort wird vielmehr klargestellt, dass auch solche Daten erfasst sein sollen, die erhoben werden, während der Nutzer inaktiv ist. Damit ist es irrelevant, ob die Daten während einer aktiven Nutzung durch den Nutzer erzeugt werden, oder ob die Daten erzeugt werden, während das Produkt oder der verbundene Dienst inaktiv, im „Stand-by“-Modus oder gar ausgeschaltet ist.[35]

Abgeleitete und aggregierte Daten fallen nicht in den Anwendungsbereich des Data Act.[36] Das Gleiche gilt für „Inhalte“.[37] Bei Inhalten handelt es sich nach den Erwägungsgründen um Text-, Audio oder visuelle Darstellungen, die häufig Rechten des geistigen Eigentums unterliegen.[38]

Im Einzelnen stellen sich hier viele Abgrenzungsfragen. Zum Beispiel ist nicht klar, wann bei vorverarbeiteten/aufbereiteten Daten die Schwelle zum „abgeleiteten Datum“ überschritten ist. Als vorverarbeitete Daten gelten Daten, „*die vor der Weiterverarbeitung und Auswertung aufbereitet wurden, um sie verständlich und nutzbar zu machen.*“[39] Aus den Erwägungsgründen ergibt sich, dass der Gesetzgeber die Grenze dort ziehen will, wo aus Daten gefolgerte bzw. abgeleitete Informationen das Ergebnis „*zusätzlicher Investitionen in die Zuweisung von Werten oder Erkenntnissen aus den Daten sind (insbesondere mittels komplexer proprietärer Algorithmen, einschließlich solcher, die Teil proprietärer Software sind*)“.[40] Der Dateninhaber soll zudem nicht verpflichtet sein, „*wesentliche Investitionen in die Bereinigung und Transformation der Daten vorzunehmen*“.[41] Wann jedoch von wesentlichen Investitionen gesprochen werden kann, bleibt offen.

Daneben beschränkt der Data Act den Datenzugangsanspruch gemäß Art. 4 Abs. 1 DA und Art. 5 Abs. 1 DA auf „ohne Weiteres verfügbare Daten“. Gemeint sind damit „*Produktdaten und verbundene Dienstdaten, die ein Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann, wobei über eine einfache Bearbeitung hinausgegangen wird*“. Auch hier stellen sich Abgrenzungsfragen.[42] Insbesondere ist unklar, wann der Dateninhaber „ohne unverhältnismäßigen Aufwand“ auf die betreffenden Produktdaten zugreifen kann.

Im Gegensatz dazu gilt der Access by Design-Anspruch gemäß Art. 3 Abs. 1 DA nicht nur für „*ohne Weiteres verfügbare Daten*“, sondern für alle „*Produktdaten*“. Bei „*Produktdaten*“ handelt es sich um „*Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – abgerufen werden können*“.[43] Diese Definition stellt wiederum nicht darauf ab, mit welchem Aufwand die Daten für den Dateninhaber zugänglich sind. Im Gegenteil – nach der Definition sind auch solche Daten als Produktdaten anzusehen, die der Hersteller so konzipiert hat, dass sie von irgendjemanden, namentlich dem Nutzer, dem Dateninhaber oder einem Dritten abrufbar sind, und zwar auch mittels physischer Verbindung.

Im Vergleich zu den Daten, die nach Art. 61 VO 2018/858 erfasst werden, sind die Daten, die dem Datenzugangsanspruch des Data Act unterliegen, in der Regel andere. Sie können sich jedoch teilweise überschneiden. Durch die Beschränkung auf Rohdaten und vorverarbeitete Daten sind die Zugangsansprüche nach dem Data Act in Bezug auf die Art der Daten enger gefasst.

Nach Art. 61 i. V. m. Art. 3 Nr. 48 der VO 2018/858 bezieht sich der Datenzugang, wie oben dargestellt, auf Reparatur- und Wartungsinformationen, unabhängig davon, in welchem Bearbeitungsstadium sich die betreffenden Daten befinden. Hier wird ein funktionaler Ansatz verfolgt,[44] indem die relevanten Daten und Informationen wie folgt definiert werden: „[S]*ämtliche Informationen, die für Diagnose, Instandhaltung und Inspektion eines Fahrzeugs, […] Reparatur […] erforderlich sind*“.[45]

Die Beschränkung der Daten und Informationen, die nach Art. 61 VO 2018/858 herauszugeben sind, erfolgt daher maßgeblich durch das Kriterium der Erforderlichkeit für den konkreten Dienst auf dem nachgelagerten Markt.

Zusammenfassend lässt sich sagen, dass der Data Act und die VO 2018/858 unterschiedliche Ansätze zum Datenzugang verfolgen. Der Data Act konzentriert sich auf Roh-

31 Hinsichtlich des Begriffs „technische Informationen“ bestehen Überlappungen mit dem Begriff der RMI-Daten. Dies ergibt sich aus der sehr breiten und offenen Definition der „technischen Informationen“ in den Kfz-Leitlinien und dem Hinweis der Kommission, dass bei der Auslegung des Begriffs auch die VO 2018/858 heranzuziehen ist und bei Vorenthaltung „technischer Reparatur- und Wartungsinformationen“ auch die Vorschriften der VO 2018/858 zu berücksichtigen sind (2023/C 133 I/01).

32 Vgl. Bekanntmachung der Kommission, 2023/C 133 I/01.

33 Zum Verhältnis des allgemeinen Kartellrechts und der Kfz-Leitlinien und der VO 2018/858 bzgl. des Zugangs zu RMI-Daten, *Hübener/Lutz*, ZWeR 2024, 130.

34 EU Kommission, Data Act Explained, https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained (Abruf: 22.7.2024).

35 ErwG 15.

36 ErwG 15.

37 Art. 1 Abs. 2 lit. a DA.

38 ErwG 16.

39 ErwG 15.

40 ErwG 15.

41 ErwG 15.

42 *Etzkorn*, RDi 2024, 116, 117; *Hennemann/Steinrötter*, NJW 2024, 1, 2.

43 Art. 2 Nr. 15 DA.

44 Studie zur Notwendigkeit und Ausrichtung von spezifischen Datenzugangsregelungen im Bereich des vernetzten Fahrzeugs in der Automobilwirtschaft – Schlussbericht, S. 80, abrufbar unter https://data.bundesnetzagentur.de/Bundesnetzagentur/DE/Fachthemen/Digitalisierung/Daten/Datenoekonomie/schlussbericht.pdf (Abruf: 22.7.2024).

45 Legaldefinition in Art. 3 Nr. 48 VO 858/2018.

daten und vorverarbeitete Daten und setzt damit engere Grenzen hinsichtlich der Art der Daten. Im Gegensatz dazu verfolgt die VO 2018/858 einen funktionalen Ansatz, der den Zugang zu allen notwendigen Informationen für Diagnose, Wartung und Reparatur eines Fahrzeugs ermöglicht, unabhängig von deren Bearbeitungsstadium. Dies führt zu einer umfassenderen Verfügbarkeit von Daten unter der VO 2018/858 im Vergleich zum Data Act.

3. In welcher Form sind die Daten/Informationen bereitzustellen?

a) Zugang zu RMI-Daten nach der VO 2018/858

Die Frage, in welcher Form RMI-Daten bereitzustellen sind, war bereits vielfach Gegenstand gerichtlicher Auseinandersetzungen.

Art. 61 Abs. 1 der VO 2018/858 bestimmt, dass RMI-Daten grundsätzlich als maschinenlesbare Datensätze in elektronisch weiterzuverarbeitender Form bereitzustellen sind.[46]

Der EuGH referenziert zur Herleitung des Begriffs der „Maschinenlesbarkeit" dabei auf die Richtlinie 2019/1024. Somit haben die Hersteller die RMI-Daten so bereitzustellen, dass eine unmittelbare elektronische Weiterverarbeitung der in den RMI-Daten enthaltenen Datensätzen möglich ist.[47]

Die RMI-Daten sind ferner grundsätzlich über Webseiten der Hersteller bereitzustellen, Art. 61 Abs. 2 der VO 2018/858. Die Ausgestaltung dieses Zugangs hat mittlerweile eine partielle Normierung über die delegierte Verordnung 2021/1244 erfahren, die etwa Informationen zur Strukturierung der Webseite bereithält.

Art. 61 Abs. 2 der VO 2018/858 sieht darüber hinaus vor, dass die Daten auch auf anderem Wege bereitgestellt werden können, wenn eine Bereitstellung über die Webseite aufgrund der Art der Informationen nicht möglich ist. Daneben steht der Zugriff auf den Fahrzeugdatenstrom über die OBD-Schnittstelle, Art. 61 Abs.1 und Abs. 4 i. V. m. Anhang X Ziffer 2.9 der VO 2018/858. Besondere Vorgaben bestehen zudem für den Zugang zu sicherheitsbezogenen RMI-Daten, für die die VO 2021/1244 das sogenannte SERMI-Scheme für anwendbar erklärt hat.

Nicht geschuldet ist hingegen ein direkte Datenbankschnittstelle zur RMI-Datenbank der Hersteller, die automatisierte Suchanfragen und Abrufe zulässt.[48] Darüber hinaus dürfte in Ermangelung konkreter Vorgaben, etwa hinsichtlich der Paketgröße von RMI-Downloads, die Ausgestaltung des Zugangs zu RMI-Daten den Herstellern überlassen sein. Grenze der Ausgestaltungsfreiheit bleiben aber stets die von der VO 2018/858 vorgegebenen Rahmenbedingungen, wie etwa die Vorgabe der leichten Zugänglichkeit der RMI-Daten, sowie die Festlegung, dass diese „*mit angemessenem Aufwand*" verarbeitet werden können, Art. 61 Abs. 2 VO 2018/858.

Diese Grenze hat der EuGH durch Vorlageentscheidungen bestätigt, in denen er jeweils ausgeführt hat, dass Hersteller gegenüber den unabhängigen Wirtschaftsakteuren keine zusätzlichen Hürden aufstellen dürfen, die nicht in der VO 2018/858 angelegt sind.[49]

b) Data Act

Im Data Act gibt es im Grunde zwei Zugangsansprüche für Nutzer. Primär soll nach Art. 3 Abs. 1 DA ein direkter Zugang zu den relevanten Produktdaten durch den Hersteller ermöglicht werden („*Access by Design*"). Wo dieser nicht gewährt werden kann, besteht ein Zugangsanspruch auf Verlangen des Nutzers gegen den Dateninhaber, Art. 4 Abs. 1 DA.

Zusätzlich kann der Nutzer vom Dateninhaber nach Art. 5 Abs. 1 DA ein Bereitstellen der Daten an einen Dritten verlangen.

(1) Zugangsansprüche des Nutzers, Art. 3 Abs.1 DA und Art. 4 Abs. 1 DA

Grundsätzlich gilt gemäß Art. 3 Abs. 1 DA, dass vernetzte Produkte so entwickelt und hergestellt werden sollen, dass die durch die Nutzung erzeugten Daten durch den Nutzer direkt zugänglich sind. Das ist ebenso bei der Erbringung verbundener Dienste zu beachten. Diese Pflicht besteht gemäß Art. 50 DA für alle nach dem 12.9.2026 in Verkehr gebrachten vernetzten Produkte und mit ihnen verbundene Dienstleistungen.

Vernetzte Produkte und verbundene Dienste müssen danach so konzipiert und hergestellt/erbracht werden, dass „*die Produktdaten und verbundenen Dienstdaten […] standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind.*"

Soweit keine direkte Zugangsmöglichkeit des Nutzers gemäß Art. 3 Abs. 1 DA besteht, greift der Zugangsanspruch nach Art. 4 Abs. 1 DA.[50]

Nach Art. 4 Abs. 1 DA „*stellen die Dateninhaber dem Nutzer ohne Weiteres verfügbare Daten […] unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit bereit. Dies geschieht auf einfaches Verlangen auf elektronischem Wege, soweit dies technisch durchführbar ist.*" Hierzu ist zunächst festzuhalten, dass die deutsche Regelung inhaltlich von der englischen und französischen abweicht.[51] Zum einen bezieht sich in den anderen Sprachfassungen die Einschränkung „*falls relevant und technisch durchführbar*"

46 Dies war unter der vorherigen Typgenehmigungsverordnung (EG) 715/2007 noch nicht geschuldet, EuGH, Urteil v. 19.9.2019 – C-527/18 – KIA Motors, GRUR 2019, 1196.

47 EuGH, Urt. v. 9.11.2023 – C-319/22, GRUR-RS 2023, 30962 (Rn. 39) – Scania, wonach etwa ein PDF-Dateiformat nicht ausreicht.

48 EuGH, Urt. v. 9.11.2023 – C-319/22, GRUR-RS 2023, 30962 (Rn. 42) – Scania.

49 EuGH Urt. v. 27.10.2022 – C-390/21 (Rn. 29, 35), BeckRS 2022, 28847; Urt. V. 5.10.2023 – C-296/22 (A. T. U. Auto-Teile-Unger GmbH & Co. KG u. Carglass GmbH/FCA Italy SpA), GRUR 2024, 62.

50 *Kaesling*, GRUR 024, 821, 823; *Hartl/Vogel*, LTZ 2024, 104, 108.

51 Englische Version: „*Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, **structured**, commonly used and machine-readable format and, **where relevant and technically feasible, continuously and in real-time**. This shall be done on the basis of a simple request through electronic means where technically feasible.*"

nur auf die Bereitstellung in Echtzeit, nicht jedoch darauf, dass die Qualität der Daten die gleiche sein muss, wie sie der Dateninhaber erhält. Es ist davon auszugehen, dass die Einschränkung im deutschen Art. 4 Abs. 1 DA ein Übersetzungsfehler ist. Andernfalls würde auch ein Bruch zwischen dem Zugangsanspruch des Nutzers in Art. 4 Abs. 1 DA und dem Anspruch auf Weitergabe dieser Daten an Dritte bestehen. Nach Art. 5 Abs. 1 DA besteht der Anspruch des Nutzers auf ein Weiterleiten an Dritte nämlich ohne Einschränkung mit gleicher Qualität wie die Daten des Dateninhabers.[52] Weshalb hier bei der Qualität zwischen den dem Nutzer selbst zugänglichen Daten und den vom Nutzer weitergeleiteten Daten unterschieden werden sollte, ist nicht ersichtlich. Daneben fehlt in der deutschen Sprachfassung der Hinweis, dass die Daten auch in „*strukturierter*" Weise zur Verfügung gestellt werden müssen. Auch hier wird man von einem Übersetzungsfehler ausgehen müssen.

Grundsätzlich soll ein Echtzeit-Zugang zu den Daten geschaffen werden.[53] Wenn dies nicht „*relevant und technisch durchführbar*"[54] ist, kann auch die Übermittlung einer Datenkopie ausreichen.[55] Jedenfalls müssen die Daten „*strukturiert, umfassend und in einem gängigen maschinenlesbaren Format*" bereitgestellt werden. Welche Formate diesbezüglich in Frage kommen, wird im Data Act nicht vorgegeben. Allerdings wird man sich hier an den Anforderungen in Art. 20 DS-GVO orientieren können und auch an den Grundsätzen,[56] die bisher in der Rechtsprechung in Bezug auf den Zugang zu RMI-Daten aufgestellt wurden. Demnach würde etwa die Bereitstellung als pdf-Datei die Voraussetzungen nicht erfüllen, da sie sämtliche Inhalte auf einer Seite gleich einem Gesamtbild wiedergeben, und die einzelnen auf einer Seite enthaltenen Daten nicht in strukturierter Weise anzeigen.[57]

(2) Zugangsanspruch zugunsten Dritter, Art. 5 Abs. 1 DA

Flankierend zu dem Anspruch nach Art. 5 Abs. 1 DA kann der Nutzer den Dateninhaber auch dazu verpflichten, die relevanten Daten direkt an einen vom Nutzer bestimmten Dritten herauszugeben. Ziel des Art. 5 Abs. 1 DA ist die Ermöglichung einer Übertragung der Daten auf Dritte, ohne dass der Nutzer diese zunächst an sich übertragen lassen muss.[58] Inhaltlich ist dieser Zugangsanspruch zugunsten des Dritten fast identisch ausgestaltet wie der Anspruch des Nutzers gegen den Dateninhaber nach Art. 4 Abs. 1 DA.[59]

Die Datenherausgabe muss zwar für den Nutzer unentgeltlich erfolgen.[60] Nach Art. 9 Abs. 1 DA kann der Dateninhaber aber eine Vergütung vom Datenempfänger für die Bereitstellung von Daten verlangen, wenn es sich um einen Datentransfer zwischen Unternehmern handelt.[61] Diese muss sich an den in Art. 9 DA festgelegten Grundsätzen orientieren.

4. Einschränkungen des Zugangsanspruchs

a) Zugang zu RMI-Daten nach der VO 2018/858

Die VO 2018/858 nennt keine Beschränkungen des Zugangs zu RMI-Daten.[62] Dies ist insoweit nicht verwunderlich, als es sich hierbei um einen sektorspezifischen Zugang für Wartungs- und Reparaturfälle handelt und damit die Zugangsregelung von vornherein nur einen begrenzten Fall abdeckt.

Durch die VO 2018/858 soll der Wettbewerb auf dem Aftersales-Markt insgesamt gefördert werden.[63] Die unabhängigen Wirtschaftsakteure und auch gerade solche, die keine unabhängigen Reparaturbetriebe sind,[64] sollen durch die Zugangsregelung befähigt werden, „*die mit ihrem Geschäft verbundenen Aufgaben in der Lieferkette des Zubehör- und Ersatzteilmarkts wahrzunehmen*", Art. 61 Abs. 2 der VO 2018/858. Der EuGH hat hierzu klargestellt, dass die VO 2018/858 unmittelbar die Möglichkeit einräumt, die bezogenen RMI-Daten zu verarbeiten und zu verwerten.[65]

Zu beachten ist ferner, dass für unterschiedliche Typen von unabhängigen Wirtschaftsakteuren teils unterschiedliche Regeln gelten, weshalb Hersteller dazu angehalten sein können, zu differenzieren. Dies gilt etwa für den Zugang zu Wartungsaufzeichnungen für unabhängige Werkstätten nach Art. 61 Abs. 9, spezifische Regelungen nach Art. 61 Abs. 2 für unabhängige Wirtschaftsakteure, die keine unabhängigen Reparaturbetriebe sind oder die Anforderungen an angemessene und verhältnismäßige, nicht abschreckende Gebühren nach Art. 63.[66] Daher verbietet sich etwa auch eine Einheitsgebühr für den Zugang zu RMI-Daten.[67]

Im Übrigen sind Beschränkungen des Zugangs zu RMI-Daten aufgrund der allgemeinen Regeln des Datenschutz- und Kartellrechts jedenfalls denkbar. Der EuGH hat jedoch bereits entschieden, dass die Zugangsregeln zu RMI-Daten nach der VO 2018/858 für Hersteller eine rechtliche Verpflichtung im Sinne des Art. 6 Abs. 1 lit. c der DSGVO darstellen, die FIN bereitzustellen.[68] Hierzu dürften jedoch noch einige Unklarheiten bestehen.[69]

b) Data Act

(1) Allgemein

Ganz allgemein stellt der Data Act klar, dass seine Regelungen nicht dazu verwendet werden dürfen, den Wettbewerb entgegen den Vorschriften des AEUV einzuschränken.[70] Dementsprechend wird vielfach darauf hingewiesen, dass das Verbot des kartellrechtlichen Informationsaustausches insbesondere bei der Herausgabe von Daten zu beachten

52 *Wiebe*, GRUR 2023, 1569, 1571.
53 Art. 4 Abs. 1 DA.
54 Art. 4 Abs. 1 DA.
55 *Hennemann/Steinrötter*, NJW 2024, 1, 3.
56 Siehe zu den Formatanforderungen etwa *Munz*, in: Taeger/Gabel, DS-GVO, 4. Aufl. 2022, Art. 20 DS-GVO Rn. 35.
57 *Munz*, in: Taeger/Gabel, DS-GVO, 4. Aufl. 2022, Art. 20 DS-GVO Rn. 38; EuGH, Urt. v. 9.11.2023 – C-319/22, GRUR-RS 2023, 30962 (Rn. 42) – Scania.
58 *Schmidt-Kessel*, MMR 2024, 75, 80.
59 *Etzkorn*, RDi 2024, 116, 121.
60 *Apel/Huber*, JuS 2024, 410, 413; *Etzkorn*, RDi 2024, 116, 121.
61 *Wiebe*, GRUR 2023, 1569, 1571; *Etzkorn*, RDi 2024, 116, 120; *Apel/Huber*, JuS 2024, 410, 413.
62 Hier ausgeklammert: Die insb. fahrzeugspezifischen Einschränkungen nach Art. 61 Abs. 3 und 10 der VO 2018/858.
63 ErwG 50f. VO 2018/858.
64 Etwa Herausgeber von technischen Informationen oder Hersteller von Ersatzteilen und Diagnosegeräten.
65 EuGH Urt. v. 27.10.2022 – C-390/21 (Rn. 29), BeckRS 2022, 28847.
66 Vgl. insbesondere zu letzterem Punkt auch EuGH Urt. v. 27.10.2022 – C-390/21 (Rn. 40), BeckRS 2022, 28847.
67 aaO.
68 EuGH, Urt. v. 9.11.2023 – C-319/22 (Rn. 62) – Scania.
69 *Hübener/Lutz*, ZWeR, 2024, 130.
70 ErwG 116.

sei.[71] In welchen Konstellationen dies in der Praxis tatsächlich relevant werden wird, ist in Anbetracht der Daten, die vom Anwendungsbereich des Data Act erfasst sind, eher fraglich. Probleme im Zusammenhang mit dem Informationsaustausch könnten sich eher in Konstellationen stellen, in denen der Dateninhaber wettbewerbssensible Daten von Nutzern erhebt oder im Zusammenhang mit dem Herausgabeverlangen strategische Informationen über Dritte erlangt, die dem Dateninhaber einen Vorteil im Wettbewerb verschaffen können.[72] Dieser Gesichtspunkt ist auch in Art. 4 Abs. 13 DA und Art. 5 Abs. 6 DA angelegt.

Anders als die VO 2018/858 führt der Data Act neben diesen allgemeinen Einschränkungen explizit noch weitere Konstellationen auf, in denen ein Zugangsverlangen verweigert werden kann.

(2) Beschränkungen beim Zugangsanspruch des Nutzers nach Art. 4 Abs. 1 DA

Art. 4 DA regelt ausdrücklich bestimmte Fälle, in denen der Dateninhaber den Zugang verweigern oder beschränken kann.

Einerseits kann der Dateninhaber den Zugriff auf die Daten verweigern, wenn es Sicherheitsbedenken gibt oder Geschäftsgeheimnisse betroffen sind.[73] Relevante Sicherheitsbedenken sind nur solche, die „*zu schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen führen*“ könnten.[74]

Geschäftsgeheimnisse können sowohl die des Dateninhabers, aber auch die von anderen Dritten sein.[75] Um diese zu schützen, sollen der Dateninhaber bzw. der Inhaber des Geschäftsgeheimnisses und der Nutzer nach Art. 4 Abs. 6 DA angemessene technische und organisatorische Maßnahmen vereinbaren, die die Vertraulichkeit der Daten wahren. Mögliche Mittel sind etwa der Abschluss von NDAs oder Verhaltenskodizes.[76] Sind diese Maßnahmen nicht ausreichend, kann der Dateninhaber gemäß Art. 4 Abs. 7 und Abs. 8 DA unter weiteren Voraussetzungen die Datenherausgabe aussetzen oder im Einzelfall ganz verweigern.[77]

Verweigert der Dateninhaber den Zugang zu den Daten aus den aufgeführten Gründen, muss er dies gemäß Art. 4 Abs. 2 und Abs. 8 DA der zuständigen Aufsichtsbehörde mitteilen.

Daneben stellt Art. 4 Abs. 12 DA für den Fall, dass es sich bei den herauszugebenden, nutzergenerierten, Daten um personenbezogene Daten handelt, klar, dass die datenschutzrechtlichen Vorschriften zu beachten sind.[78] Ist der Nutzer, der das Zugangsverlangen geltend macht, gleichzeitig die betroffene Person i. S. d. DSGVO, kann der Verantwortliche die Herausgabe der personenbezogenen Daten auf eine ausreichende Rechtsgrundlage im Sinne des Art. 6 DSGVO bzw. Art 9 DSGVO (je nach Konstellation) stützen. Ist der Nutzer nicht die betroffene Person, muss gemäß Art. 5 Abs. 7 DA ein Erlaubnistatbestand nach Art. 6, 9 DSGVO vorliegen und gegebenenfalls die Bedingungen des § 25 TDDDG erfüllt sein, damit die Daten bereitgestellt werden können.[79] Liegen diese nicht vor, kann die Herausgabe der Daten verweigert werden.

Die FIN stellt nach Auffassung des EuGH ein personenbezogenes Datum dar, wenn eine natürliche Person im Fahrzeugschein als Halter eingetragen ist. Dies gilt jedoch nur dann, wenn die Person, die Zugang zur FIN hat, auch die Möglichkeit hat, die natürliche Person, auf die sich die FIN bezieht, zu identifizieren.[80] Dementsprechend sind nutzergenerierte Daten, die mit der FIN verknüpft sind, oftmals als personenbezogene Daten anzusehen und daher bei deren Herausgabe die datenschutzrechtlichen Vorgaben einzuhalten.

Auch soweit die datenschutzrechtlichen Grundlagen für eine Weitergabe der personenbezogenen Daten nicht vorliegen, heißt das jedoch nicht, dass die Datenherausgabe in diesen Fällen gänzlich verweigert werden kann. Aus Erwägungsgrund 7 ergibt sich, dass „*der Dateninhaber Datenzugangsverlangen in diesen Fällen unter anderem nachkommen [kann], indem er personenbezogene Daten anonymisiert oder, wenn ohne Weiteres verfügbare Daten personenbezogene Daten mehrerer betroffener Personen enthalten, nur personenbezogene Daten des Nutzers übermittelt*“.

(3) Beschränkungen bei Access by Design nach Art. 3 Abs. 1 DA

Beim Datenzugang nach Art. 3 DA erhält der Nutzer Zugang zu den Daten mittels der vom Dateninhaber geschaffenen Schnittstelle. Der Datenzugang scheint daher eher auf rein faktischer Basis zu erfolgen.[81]

Weitergehenden Einschränkungen unterliegt der Zugang nach Art. 3 Abs. 1 DA nach dem Gesetzestext nicht. Insbesondere fehlt eine Bezugnahme auf die in Art. 4 DA vorgesehenen Tatbestände.[82] Eine analoge Anwendung wird mangels Regelungslücke wohl eher verneint.[83]

Dies führt im Ergebnis dazu, dass der Nutzer über Art. 3 Abs. 1 DA einen gänzlich unbeschränkten Zugang zu den Daten, und damit auch z. B. zu Geschäftsgeheimnissen des Dateninhabers (und auch möglicherweise Dritter) oder personenbezogenen Daten von Dritten erhalten könnte. Gerade vor dem Hintergrund, dass der Data Act ausdrücklich klarstellt, dass „*keine Bestimmung dieser Verordnung […] dahingehend angewandt oder ausgelegt werden [sollte], dass das Recht auf den Schutz personenbezogener Daten […] abgeschwächt oder eingeschränkt wird*“,[84] erscheint dieses Verständnis etwas weitgehend. Ob dies wirklich so gewollt ist oder ob nicht vielmehr z. B. durch die Einrichtung von Nutzeraccounts auch im Falle des Zugangsanspruchs nach Art. 3 Abs. 1 DA gewisse (vertragliche) Schranken eingeführt werden sollten, ist unklar.

In den Erwägungsgründen wird in Bezug auf vernetzte Produkte, bei denen typischerweise mehrere Personen als Nutzer gelten, festgestellt, dass deren „*Konzeption […] oder [die Konzeption] der entsprechenden Schnittstelle jedem Nutzer den Zugang zu den von diesen generierten Daten ermöglichen*“ soll.[85] Dadurch könne zum Beispiel

71 *Heinzke/Herbers/Kraus*, BB 2024, 649, 653 f.
72 *Wiebe*, GRUR 2023, 1569, 1571.
73 Art. 4 Abs. 2, 7 DA.
74 Art. 4 Abs. 2 S. 1 DA.
75 *Hennemann/Steinrötter*, NJW 2024, 1, 3.
76 Hierzu ausführlich *Heinzke/Herbers/Kraus*, BB 2024, 649, 653.
77 Art. 4 Abs. 8 DA; *Hennemann/Steinrötter*, NJW 2024, 1, 4.
78 ErwG 34.
79 *Hennemann/Steinrötter*, NJW 2024, 1, 4.
80 EuGH, Urt. v. 9.11.2023 – C-319/22 (Rn. 48 f.) – Scania
81 *Heinzke/Herbers/Kraus*, BB 2024, 649, 652.
82 *Schmidt-Kessel*, MMR 2024, 75, 80.
83 *Schmidt-Kessel*, MMR 2024, 75, 80.
84 ErwG 7.
85 ErwG 21.

die Identifizierung des Nutzers sichergestellt werden.[86] Ob diese Ausführungen auch für den Access by Design-Anspruch gelten oder sich allein auf den Herausgabeanspruch nach Art. 4 Abs. 1 DA beziehen, geht aus den Erwägungsgründen nicht eindeutig hervor. Der Umstand, dass auch Art. 3 Abs. 1 DA grundsätzlich nur regelt, dass die Daten für den Nutzer (und nicht für jeden) direkt zugänglich sein sollen, könnte eher für die Einrichtung von Nutzeraccounts sprechen. Dies insbesondere dann, wenn das vernetzte Produkt typischerweise von mehreren Nutzern genutzt wird.

(4) Beschränkungen beim Zugangsanspruch zugunsten Dritter nach Art. 5 Abs. 1 DA

Der Zugangsanspruch des Dritten unterliegt den Beschränkungen nach Art. 5 Abs. 9 bis Abs. 12 DA. Diese sind weitgehend parallel zu den Beschränkungen des Zugangsanspruches des Nutzers.[87] Zusätzlich hat der Nutzer gemäß Art. 5 Abs. 2 DA keinen Anspruch darauf, dass „*Daten im Zusammenhang mit der Prüfung neuer vernetzter Produkte, Stoffe oder Verfahren, die noch nicht in Verkehr gebracht werden*“ an Dritte bereitgestellt werden.

5. Verwendungsbeschränkungen in Bezug auf die Daten

a) Zugang zu RMI-Daten

Wenngleich auch nicht ausdrücklich im Wortlaut der Art. 61 f. der VO 2018/858 festgelegt, scheint jedoch im Umkehrschluss eine Begrenzung der Nutzung von RMI-Daten auf Geschäftsfelder im Aftersales-Bereich im Binnenmarkt (im weitesten Sinne)[88] nicht gänzlich ausgeschlossen zu sein. Dafür spricht vor allem der Sinn und Zweck der Zugangsregelung, die darauf ausgerichtet ist, den Wettbewerb zwischen unabhängigen Wirtschaftsakteuren, autorisierten Betrieben und Herstellern im Aftersales-Bereich weiter zu beleben.[89]

b) Data Act

Der Data Act enthält einige ausdrückliche Verwendungsbeschränkungen in Bezug auf die Daten.

So darf der Nutzer gemäß Art. 4 Abs.10 DA die Daten nicht nutzen, um ein vernetztes Produkt zu entwickeln, das mit dem Produkt, das die Daten generiert hat, im Wettbewerb steht. Daneben ist zudem die Weitergabe der Daten an einen Dritten oder die eigene Nutzung zur Erlangung eines Einblicks in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers des vernetzten Produkts bzw. des Dateninhabers unzulässig (Art. 4 Abs. 10, 2. Alt. 2 DA). Der Nutzer darf den Hersteller bzw. Dateninhaber also nicht mittels der erlangten Daten ausspähen.[90] Ein spiegelbildliches Verbot gilt für den Dateninhaber nach Art. 4 Abs. 13 DA.[91]

Für den Dritten, der Daten auf Verlangen des Nutzers erhält, sieht Art. 6 DA gleich eine ganze Reihe von ausdrücklichen Beschränkungen in Bezug auf die erhaltenen Daten vor. Soweit ein Dritter Daten auf Verlangen eines Nutzers erhält, unterliegt er den Vorgaben in Art. 6 DA.[92] Insbesondere darf der Dritte die herausgegebenen Daten nur im Rahmen der vertraglichen Vereinbarung mit dem Nutzer verwenden, Art. 6 Abs. 1 DA.[93]

Daneben gilt auch für den Dritten das Verbot, die Daten zu verwenden, um ein Wettbewerbsprodukt herzustellen oder den Dateninhaber bzw. Hersteller „auszuspähen“, Art. 6 Abs. 2 lit. e DA. Der Dritte darf die Daten ferner nicht für ein Profiling verwenden, Art. 6 2 lit. b DA, oder sie einem anderen Dritten bereitstellen, soweit dies nicht ausdrücklich mit dem Nutzer vereinbart ist, Art. 6 Abs. 2 lit. c DA. Er darf die Daten auch keinem Gatekeeper bereitstellen, Art. 6 Abs. 2 lit. d DA, oder sie so nutzen, dass dies nachteilige Auswirkungen auf die Sicherheit des vernetzten Produkts oder des verbundenen Dienstes hat, Art. 6 Abs. 2 lit. f DA. Darüber hinaus hat er die vereinbarten Maßnahmen zur Vertraulichkeit bzw. zur Wahrung von Geschäftsgeheimnissen zu beachten, Art. 6 Abs. 2 lit. g DA.

6. Zwischenfazit

Der Vergleich der Datenzugangsansprüche nach der VO 2018/858 und dem Data Act offenbart sowohl Überschneidungen als auch deutliche Unterschiede in ihren Ansätzen und Zielsetzungen. Der Data Act verfolgt einen breiteren, nutzerzentrierten Ansatz, während die VO 2018/858 funktionsorientierte, sektorspezifische Zugangsrechte etabliert.

Die sektorspezifischen Zugangsregeln der VO 2018/858 betreffen vor allem den Zugang zu RMI-Daten, die für Wartung und Reparatur erforderlich sind. Ziel ist es – auch durch die zudem bestehenden Zugänge zu OBD-Daten, Werkzeugen und sonstigen Geräten – den unabhängigen Aftersalesmarkt im Wettbewerb mit autorisierten Betrieben und Herstellern zu ertüchtigen.

Der Data Act statuiert Zugangsregeln und -ansprüche für nutzergenerierte Daten u. a. in Fahrzeugen. Bezüglich der Art der relevanten Daten verfolgt der Data Act dabei einen engeren Ansatz, indem er sich auf Rohdaten und vorverarbeitete Daten konzentriert, ohne jedoch weitere Einschränkungen hinsichtlich der Inhalte dieser Daten zu normieren. In Einzelfällen ist es dennoch denkbar, dass bestimmte RMI-Daten unter die Zugangsregeln der VO 2018/858 und des Data Act fallen.

Die RMI-Zugangsregeln der VO 2018/858 richten sich direkt an unabhängige Wirtschaftsakteure als Zugangsberechtigte, damit diese ihrer Funktion im Aftersalesmarkt nachkommen können. Demgegenüber stellt der Data Act den Nutzer in den Mittelpunkt und räumt Dritten, wie etwa unabhängigen Wirtschaftsakteuren, nur einen abgeleiteten Zugangsanspruch ein, soweit diese nicht (ausnahmsweise) selbst Nutzer sind.

Ein weiterer Unterschied besteht hinsichtlich der möglichen Ablehnung eines Zugangsverlangens. Während die VO 2018/858 hierzu keine spezifischen Bestimmungen enthält, führt der Data Act explizit bestimmte Konstellationen auf, in denen ein Zugangsverlangen verweigert oder die Nutzung der Daten beschränkt werden kann.

86 ErwG 21.
87 *Schmidt-Kessel* MMR 2024, 75, 81; *Heinzke/Herbers/Kraus*, BB 2024, 649, 654.
88 Vgl. etwa RMI-Bericht der Kommission v. 9.12.2016, COM (2016) 782 final (Ziffer 3).
89 Vgl. ErwG 50, 52 und Art. 61 Abs. 2 der VO 2018/858.
90 *Heinzke/Herbers/Kraus*, BB 2024, 649, 654.
91 *Herbers/Kraus*, BB 2024, 649, 654.
92 *Götz/Blöink*, MMR 2024. 451, 452.
93 *Apel/Huber*, JuS 2024 410, 413.

III. Auswirkungen des Data Act auf den Zugangsanspruch bzw. Vertragsverhältnisse in Zusammenhang mit dem Zugang und der Nutzung von RMI-Daten

Da der Data Act „harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung" regeln soll, geht er in seinem Anwendungsbereich wesentlich weiter, als es die Datenzugangsansprüche in Kapitel II vermuten lassen. Insbesondere in den Kapitel III und IV enthält der Data Act zahlreiche Vorschriften, die zukünftig auch für sektorspezifische Datenzugangsansprüche und ganz allgemein, für Verträge im Zusammenhang mit der Datennutzung und-weitergabe relevant sein werden.

1. Auswirkungen der FRAND-Vorgaben auf Zugangsansprüche zu RMI-Daten

Kapitel III des DA, namentlich Art. 9–11 DA, enthalten Regelungen zum fairen, angemessenen und diskriminierungsfreien Datenzugang sowie zu einer angemessenen Vergütung (FRAND-Vorgaben). Die Regelungen gelten immer dann, wenn ein Dateninhaber verpflichtet ist, Daten nach dem Unionsrecht bzw. nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsakten bereitzustellen.[94]

Für bereits bestehende Rechtsakte stellt der Data Act jedoch klar, dass diese von den Vorgaben des Kapitels III grundsätzlich unberührt bleiben.[95] Dementsprechend finden die FRAND-Vorgaben, die an einigen Stellen etwas enger scheinen, als die Vorgaben in Art. 63 VO 2018/858, zunächst einmal keine direkte Anwendung auf die Zugangsverlangen in Bezug auf RMI-Daten.[96] Es ist allerdings davon auszugehen, dass eine zukünftige Neufassung der VO 2018/858 die Vorgaben in Kapitel III entsprechend übernehmen wird.[97]

Darüber hinaus ist nicht auszuschließen, dass Kapitel III des Data Act bei der Interpretation noch offener Fragen in Bezug auf die Herausgabe von RMI-Daten durchaus relevant werden könnte.

2. Auswirkungen des Data Act auf Datenlizenzverträge im Zusammenhang mit dem bzw. der Nutzung von RMI-Daten

Der Data Act enthält in Kapitel IV dezidierte Regelungen zu missbräuchlichen Vertragsklauseln und damit eine dem deutschen Recht sehr ähnliche Inhaltskontrolle im B2B-Bereich. Diese Regelungen finden auf jede Vereinbarung Anwendung, die den Datenzugang bzw. die Datennutzung zum Gegenstand hat oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten, soweit die betreffende Klausel einseitig gestellt wurde.[98] Sie gelten daher nicht nur, soweit ein Zugangsanspruch zu diesen Daten besteht, sondern immer dann, wenn Gegenstand eines Vertrags zwischen Unternehmen die Datennutzung bzw. der Datenzugang ist.

Art. 13 DA findet daher auch auf solche Verträge Anwendung, die Hersteller beispielsweise mit unabhängigen Marktteilnehmern etc. in Bezug auf die Bereitstellung von RMI-Daten abgeschlossen haben, soweit, was in der Praxis die Regel sein dürfte, diese Verträge einseitig von den Herstellern vorgegeben werden.

Bei der konkreten Ausgestaltung solcher Verträge ist demnach zukünftig Art. 13 DA zu berücksichtigen. Danach sind „*Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten, die ein Unternehmen einem anderen Unternehmen einseitig auferlegt, [..] für letzteres Unternehmen nicht bindend, wenn sie missbräuchlich sind*", Art 13 Abs. 1 DA. Nach der Generalklausel des Art. 13 Abs. 3 DA ist dies etwa bei einer „*groben Abweichung von der guten Geschäftspraxis*" oder einem Verstoß „*gegen das Gebot von Treu und Glaube*n" der Fall. Dies wird in den Absätzen 4 und 5 mit entsprechenden Regelbeispielen näher konkretisiert.

Kapitel IV gilt auch für bestehende Verträge, sodass diese an die betreffenden Vorgaben in Art. 13 DA angepasst werden sollten. Allerdings sieht der Data Act in Bezug auf bestehende Verträge zumindest eine Übergangsphase vor. Danach gilt Kapitel IV erst ab dem 12.9.2027 für Verträge, die am oder vor dem 12.9.2025 geschlossen wurden und dies auch nur für bestimmte Altverträge.[99]

IV. Fazit

Im Automotivebereich gibt es mittlerweile zahlreiche Zugangsregeln zu Daten. Die hier verglichenen Regelwerke richten sich beide im Ergebnis an OEMs. Während die RMI-Zugangsregeln der VO 2018/858 primär aus kartellrechtlichen Überlegungen entwickelt wurden, um bestimmten Marktteilnehmern den Zugang zu notwendigen Daten für die Bereitstellung von Dienstleistungen und Produkten auf nachgelagerten Märkten zu ermöglichen, verfolgt der Data Act einen breiteren Ansatz. Der Data Act gewährt Nutzern eines bestimmten Produkts das Recht auf die Daten, die bei der Nutzung dieses Produkts generiert wurden, und normiert darüber hinaus einen Anspruch auf Weitergabe dieser Daten an Dritte. Der Vergleich der Datenzugangsansprüche gemäß der VO 2018/858 und dem Data Act zeigt sowohl Gemeinsamkeiten als auch signifikante Unterschiede in ihren Ansätzen und Zielsetzungen auf.

Neben den spezifischen Regelungen zum Zugang zu nutzergenerierten Daten enthält der Data Act auch weitergehende Bestimmungen, die im Zusammenhang mit der Weitergabe von RMI-Daten relevant werden können. So beinhaltet der Data Act unter anderem allgemeine Regeln für die Ausgestaltung von Zugangsansprüchen auf Grundlage des Unionsrechts sowie für die Ausgestaltung von Datennutzungs- und Datenzugangsverträgen. Letztere haben unmittelbare Relevanz auch für bestehende Verträge, die beispielsweise die Nutzung von RMI-Daten regeln. Es bleibt darüber hinaus abzuwarten, ob die Regelungen in Kapitel III, die konkrete Vorgaben für die Ausgestaltung von Zugangsansprüchen vorsehen, mittelbar auch Auswirkungen auf den Zugang zu RMI-Daten haben werden.

94 Art 12 Abs. 1 DA.
95 Art 44 DA sowie Art 50 DA.
96 Vgl. zu den Gebühren für Zugang zu RMI-Daten, *Hübener/Lutz*, ZWeR 2024, 130.
97 EU Kommission, Data Act Explained, https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained, Chapter III (Abruf: 22.7.2024).
98 Art 13 Abs. 1 DA.
99 Art 50 DA; Es sind nur solche Altverträge betroffen, die unbefristet abgeschlossen wurden oder die frühestens 10 Jahre nach dem 11 Januar 2024 enden.